UNCLASSIFIED

Leg
OCA 2251-89

17 July 1989

NOTE FOR: [redacted] STAT
Legislative Officer
Legislation Division/Office of Congressional Affairs

FROM: [redacted] STAT
Assistant General Counsel
Intelligence Law Division

SUBJECT: Pending Electronic Surveillance Bills

1. Attached are materials pertaining to the bills regarding electronic surveillance, that we discussed last week. The Agency appears to have significant equities which could be effected by provisions in each bill. Please keep me informed of the status of these bills. We will probably want to chime in with our concerns, when appropriate. [redacted]

[redacted]

STAT

[redacted]

STAT

UNCLASSIFIED

STAT

101ST CONGRESS
1ST SESSION

H. R. 2168

To prevent potential abuses of electronic monitoring in the workplace.

IN THE HOUSE OF REPRESENTATIVES

MAY 2, 1989

Mr. CLAY (for himself, Mr. EDWARDS of California, Mr. WILLIAMS, and Mr. GILMAN) introduced the following bill; which was referred to the Committee on Education and Labor

---

A BILL

To prevent potential abuses of electronic monitoring in the workplace.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Privacy for Consumers and Workers Act".

SEC. 2. DEFINITIONS.

As used in this Act—

(1) the term "electronic monitoring" means the collection, storage, analysis, and reporting of information concerning an employee's activities by means of a

computer, electronic observation and supervision, remote telephone surveillance, telephone call accounting, or other form of visual, auditory, or computer-based surveillance conducted by any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system;

(2) the term "employee" means any current or former employee of an employer;

(3) the term "employer" means any person who employs employees, and includes any individual, corporation, partnership, labor organization, unincorporated association, or any other legal business, the Federal Government, any State (or political subdivision thereof), and any agent of the employer;

(4) the term "personal data" means any information concerning an employee which, because of name, identifying number, mark, or description, can be readily associated with a particular individual, and such term includes information contained in printouts, forms, or written analyses or evaluations;

(5) the term "prospective employee" means an individual who has applied for a position of employment with an employer; and

(6) the term "Secretary" means the Secretary of Labor.

SEC. 3. NOTICE.

(a) IN GENERAL.—Each employer who engages in electronic monitoring shall provide each affected employee with prior written notice describing the following regarding the electronic monitoring directly affecting the employee:

(1) The forms of electronic monitoring to be used.

(2) The personal data to be collected.

(3) The frequency of each form of electronic monitoring which will occur.

(4) The use of personal data collected.

(5) Interpretation of printouts of statistics or other records of information collected through electronic monitoring.

(6) Existing production standards and work performance expectations.

(7) Methods for determining production standards and work performance expectations based on electronic monitoring statistics.

(b) NOTICE CONCERNING EXISTING FORMS OF ELECTRONIC MONITORING.—(1) Each employer shall notify a prospective employee at any personal interview or meeting of existing forms of electronic monitoring which may directly

affect the prospective employee if such employee is hired by the employer.

(2) Each employer, upon request by a prospective employee, shall provide the prospective employee with the written notice described in subsection (a) regarding existing forms of electronic monitoring which may directly affect the prospective employee if such employee is hired by the employer.

(3) Each employer who engages in electronic monitoring shall provide the affected employee with a signal light, beeping tone, verbal notification, or other form of visual or aural notice, at periodic intervals, that indicates that electronic monitoring is taking place. If the electronic monitoring is conducted on a continuous basis during each of the employee's shift, such notice need not be provided at periodic intervals.

(4) An employer who engages in telephone service observation shall provide the affected customer with a signal light, beeping tone, verbal notification, or other form of visual or aural notice, at periodic intervals, indicating that the telephone service observation is taking place.

(c) NOTICE TO CURRENTLY AFFECTED EMPLOYEES.—Notwithstanding subsection (a), an employer who is engaged in electronic monitoring on the effective date of this Act shall have 90 days after such date to provide each affected employee with the required written notice.

SEC. 4. ACCESS TO RECORDS.

Each employer shall permit an employee (or the employee's authorized agent) to have access to all personal data obtained by electronic monitoring of the employee's work.

SEC. 5. PRIVACY PROTECTIONS.

(a) RELEVANCY REQUIRED.—An employer shall not collect personal data on an employee through electronic monitoring which is not relevant to the employee's work performance.

(b) DISCLOSURE LIMITED.—An employer shall not disclose personal data obtained by electronic monitoring to any person or business entity except to (or with the prior written consent of) the individual employee to whom the data pertains, unless the disclosure would be—

(1) to officers and employees of the employer who have a legitimate need for the information in the performance of their duties;

(2) to a law enforcement agency in connection with a criminal investigation or prosecution; or

(3) pursuant to the order of a court of competent jurisdiction.

SEC. 6. USE OF OF DATA COLLECTED BY ELECTRONIC MONITORING.

(a) DATA MAY NOT BE USED AS SOLE BASIS FOR EVALUATION.—An employer shall not use personal data obtained by electronic monitoring as the exclusive basis for indi-

vidual employee performance evaluation or disciplinary action, unless the employee is provided with an opportunity to review the personal data within a reasonable time after such data is obtained.

(b) DATA MAY NOT BE USED AS SOLE BASIS FOR PRODUCTION QUOTAS.—An employer shall not use personal data or collective data obtained by electronic monitoring data as the sole basis for setting production quotas or work performance expectations.

(c) DATA MAY NOT DISCLOSE EMPLOYEE'S EXERCISE OF CONSTITUTIONAL RIGHTS.—An employer shall not maintain, collect, use, or disseminate personal data obtained by electronic monitoring which describes how an employee exercises rights guaranteed by the First Amendment unless such use is expressly authorized by statute or by the employee to whom the data relates or unless pertinent to and within the scope of, an authorized law enforcement activity.

SEC. 7. ENFORCEMENT PROVISIONS.

(a) CIVIL PENALTIES.—(1) Subject to paragraph (2), any employer who violates any provision of this Act may be assessed a civil penalty of not more than $10,000.

(2) In determining the amount of any penalty under paragraph (1), the Secretary shall take into account the previous record of the person in terms of compliance with this Act and the gravity of the violation.

(3) Any civil penalty assessed under this subsection shall be collected in the same manner as is required by subsections (b) through (e) of section 503 of the Migrant and Seasonal Agricultural Worker Protection Act (29 U.S.C. 1853) with respect to civil penalties assessed under subsection (a) of such section.

(b) INJUNCTIVE ACTIONS BY THE SECRETARY.—The Secretary may bring an action under this section to restrain violations of this Act. The Solicitor of Labor may appear for and represent the Secretary in any litigation brought under this Act. In any action brought under this section, the district courts of the United States shall have jurisdiction, for cause shown, to issue temporary or permanent restraining orders and injunctions to require compliance with this Act, including such legal or equitable relief incident thereto as may be appropriate, including employment, reinstatement, promotion, and the payment of lost wages and benefits.

(c) PRIVATE CIVIL ACTIONS.—(1) An employer who violates this Act shall be liable to the employee or prospective employee affected by such violation. Such employer shall be liable for such legal or equitable relief as may be appropriate, including employment, reinstatement, promotion, and the payment of lost wages and benefits.

(2) An action to recover the liability prescribed in paragraph (1) may be maintained against the employer in any

Federal or State court of competent jurisdiction by an employee or prospective employee for or on behalf of such employee, prospective employee, and for other employees or prospective employees similarly situated. No such action may be commenced more than 3 years after the date of the alleged violation.

(3) The court, in its discretion, may allow the prevailing party (other than the United States) reasonable costs, including attorney's fees.

(d) WAIVER OF RIGHTS PROHIBITED.—The rights and procedures provided by this Act may not be waived by contract or otherwise, unless such waiver is part of a written settlement agreed to and signed by the parties to the pending action or complaint under this Act.

SEC. 8. REGULATIONS.

The Secretary shall, within 6 months after the date of the enactment of this Act, issue rules and regulations to carry out the provisions of this Act.

SEC. 9. INAPPLICABLE TO MONITORING CONDUCTED BY LAW ENFORCEMENT AGENCIES.

This Act shall not apply to electronic monitoring administered by law enforcement agencies as may otherwise be permitted in criminal investigations

STAT

○

WASHINGTON POST
NEW YORK TIMES
WALL STREET J.
WASHINGTON TIMES F2
USA TODAY

DATE 11 JULY 89

ILLEGIB

A real right to privacy

The House of Representatives has a chance to strengthen a right of privacy that all of us understand: the right not to be victimized by wiretapping or eavesdropping. Rep. Ronald Dellums has submitted a "Privacy Assurance Act of 1989," which would forbid private citizens from snooping on one another unless both parties consented or unless one party had received a court's permission to eavesdrop on the affairs of the other.

The bill would force all states to adopt the doctrine of "two-party consent." Surprisingly, many states and the District of Columbia permit people to eavesdrop on others without having to seek the consent of those being photographed or recorded. This newspaper's recent stories about a local prostitution ring includes at least one lurid example of this practice. Lobbyist Craig Spence reportedly lured acquaintances into his bugged house, invited them to frolic with prostitutes and used tapes of the events to blackmail them. Local court dockets also include plenty of cases in which businessmen snooped on one another, parties to a divorce used recordings in order to coerce favorable settlements from one another and businessmen tried to engage in various forms of industrial espionage.

The Dellums bill attempts to outlaw unauthorized snooping and impose reasonable standards of honor and decency in private conversations and transactions. It forbids the unauthorized sale of bugging devices, requires that voice-activated recorders emit "beeps" audible to the people being recorded and demands that manufacturers stamp recording devices with labels that outline the provisions of the law. The measure applies to devices "virtually certain" to be used for the "surreptitious interception of communications."

The bill promotes the kind of privacy right that most people understand, the right to speak freely and openly in private, without fear that their words will be used against them or twisted in ways that place their reputations or lives at risk. It also tries to ensure that people who don't have the decency to get a person's permission to record a conversation or activity will be liable for civil fines.

The measure, House Resolution 2551, represents an important attempt to defend people's individual rights against technologies that may be used to restrict those rights. Congress ought to advance that principle of privacy while taking care that the bill not be twisted to absurd extremes, such as outlawing diary entries or requiring all voice-activated recorders to have "beepers." While the Constitution creates no right to extortion and the Framers never intended to make the First Amendment supreme over all others, Americans also have learned that imprecise legislative language sometimes can create more problems than it prevents.

The Dellums bill needs work if it is to preserve individual privacy without placing absurd restrictions on free expression. Properly refined, the bill would enable people to speak freely, knowing that nothing short of a court order would permit friends or foes from using their words or deeds against them.

The federal government has expressed interest in the technology, he said, but no formal contracts have been signed or planned. "People approach you at conferences or conventions, tell you they're with the government and have heard about the technology," Carlson said. He didn't know which government agencies were interested, but said government interest in such a widely applicable technology was not suprising. He did not think the technology could conceivably be used for surveilance in the near future.

The technology does not record the image and in terms of surveillance, Carlson say it "will never be as good as one that records the image," he said. "That's the stuff to watch out for."

John A. Dimling, a Nielsen vice president, played down privacy concerns. "We're not scanning the room to find out what people are doing. We're sensitive to the issue of privacy." Carlson conceded that as the technology becomes more sophisticated it could open up more questions of privacy.

Ted Leventhal

CANADIAN REPORT: CAPA TO SPONSOR
FIRST DEBATE ON ACCESS STATUTE

The Canadian Access and Privacy Association (CAPA) will hold its first public event -- a June 28 discussion entitled "Access to Information Act: Six Years Old or Six Years Under?"

The forum will feature Stephen Bindman, president of the Center for Investigative Journalism, Professor William Kaplan, of the Univ. of Ottawa School of Law, David McKendry, of the Canadian Consumers' Association, Pierre Beaudry, of Supply and Services Canada, Jacqueline Bilodeau, of Environment Canada and two speakers to be announced later.

For more information, contact: (613) 990-4136.

Medical Databases. Medical informatics specialists must adopt a code of ethics and other safeguards because electronic databases can becomes a means of spying, warned Elke-Henner Kluge, a University of Victoria professor of ethics, at a May 17 conference.

There must be safeguards and patient consent if a privacy health record is exposed through electronic means, Kluge said. "Nothing is as intimate as the data package describing you as you enter a health care setting." Accessing the data without consent, he added, would be the equivalent of "electronic assault."

Kluge presently is working on a code of ethics for computing professionals in health care. Starting July 1, he will serve one year in Ottawa as director of the division of ethics and legal affairs of the Canadian Medical Association.

DELLUMS INTRODUCES AMENDMENTS TO EAVESDROPPING
LAWS; POSTAL SERVICE TO REVIEW REGULATIONS

Rep. Ron Dellums (D-Calif.) has introduced a bill that would strengthen Federal eavesdropping laws.

Dellum's amendments would close the "one party consent" rules presently providing for individuals to tape their phone calls without the other party's knowledge.

The bill amends section 2511(2)(d) of title 18, United States Code. "It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where all parties to the communication have given prior consent to such interception."

The legislation adds new regulations for the sale of voice-activated tape recorders. The bill requires that all voice-activated recorders create a beep-tone when activated and that every recorder display a warning label indicating legal prohibitions and penalties.

Meanwhile, Pittsburgh radio journalist Rudolph Brewington's complaint to the Postal Service concerning mail-order surveillance devices has elicited a review of regulations from Chief Postal Inspector Charles R. Clauson.

Brewington and Robert Moore Jr. have produced a report "Domestic Surveillance: America's Dirty Little Secret," (Privacy Times, January 23). Brewington and Moore note that Title 18 outlaws surveillance, but that the protection is weakened severely by the so called one-party consent exception, which allows one person engaged in a conversation to secretly record the other person.

Because of the this loophole, they write, "The ability of average citizens to 'bug' each other actually exceeds that of law enforcement officials who can conduct surveillance only under strict court procedures....

"Using the one party consent loophole, and by inserting false and misleading disclaimers in their advertisements-- claiming that the responsibility of complying with the law is on the buyer, not the seller -- and due to a lack of enforcement of the law by officials -- many who are themselves ignorant of the law -- a multimillion dollar industry has developed, resulting in a flood of illegal products on the market, wholesale violations of privacy, and a growing willingness of individuals -- particularly in divorce actions, to use the devices," they write.

Ted Leventhal

FOIA CT. ROUNDUP: PERSONAL BUSINESS PARTNERS; INS WATCHLIST ON CANADIANS

The following is a summary of recent court decisions under the Freedom of Information Act.

Dow Jones & Company v. General Services Administration, et al.: (No. 88-0686)

Court:	U.S. District Court for the District of Columbia
Judge:	Charles R. Richey
Document:	List of business partners of former GSA Administrator T. Golden
Issue:	Whether list created by Golden is an "agency record"
Decided:	June 7, 1989

The court ruled that a list of business partners compiled of then GSA Administrator Terrence Golden and maintained in a locked safe did not constitute an agency record and therefore did not have to be disclosed under the Freedom of Information Act.

The list of business partners was compiled by Golden's accountant at his own expense in response to a congressional committee's concerns that his ex-